UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/761,499	01/16/2001	Mark Ontiveros	CAPTNE/P002A1	5908

				EXAMINER
29914	7590	04/21/2004		EL CHANTI, HUSSEIN A

DKW LAW GROUP, P.C.
58TH FLOOR - USX TOWER
600 GRANT STREET
PITTSBURGH, PA 15219

ART UNIT	PAPER NUMBER
2157	7

DATE MAILED: 04/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/761,499 **Applicant(s)** ONTIVEROS ET AL.
	Examiner Hussein A El-chanti **Art Unit** 2157

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _16 January 2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _16 January 2001_ is/are: a)☐ accepted or b)☒ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All   b)☐ Some *   c)☐ None of:

       1.☐ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _6_.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to application filed on Jan. 16, 2001. Claims 1-20 are

pending examination.

Drawings

2.   Formal Drawings are required to be submitted by applicant.

Claim Objections

3.   *A series of singular dependent claims is permissible in which a dependent claim*

refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any

claim which does not also depend from said dependent claim. It should be kept in mind

that a dependent claim may refer to any preceding independent claim. In general,

applicant's sequence will not be changed. See MPEP § 608.01(n).

Claim 6 is dependent on claim 3 and separated by claims 4 and 5.

4.   Claim 1 is objected to because of the following informalities:

The seventh line of the claim states "form". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5.   Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by

Cunningham et al., U.S. Patent No. 6,219,786 (referred to hereafter as Cunningham).

As to claim 1, Cunningham teaches a method of protecting a network from

potentially harmful data traffic traversing a plurality of data ports of the network, the data

traffic comprising data packets, the method comprising the steps of:

monitoring all the data packets traversing the data ports from a plurality of

sources (see col. 3 lines 56-col. 4 lines 5);

determining the number of data packets form each source traversing the data

ports during a predetermined period of time (see col. 9 lines 1-12); and

denying access to the data ports to data packets from a particular source if the

number of packets traversing the ports from that source is greater than a predetermined

number during the predetermined period of time (see col. 9 lines 1-12).

As to claim 2, Cunningham teaches the method according to claim 1 wherein the

step of denying access to the source is automatic (see col. 9 lines 1-12).

As to claim 3, Cunningham teaches the method according to claim 1 further

comprising the step of copying each of the data packets for monitoring (see col. 7 lines

56-col. 8 lines 8).

As to claim 4, Cunningham teaches the method according to claim 1 wherein the

step of monitoring further comprises monitoring both incoming and outgoing data

packets traversing the data ports (see col. 4 lines 31-44).

As to claim 5, Cunningham teaches the method according to claim 1 where the step of monitoring further comprises separately monitoring the data packets traversing each of the data ports (see col. 10 lines 1-20).

As to claim 6, Cunningham teaches the method according to claim 3 further comprising using protocol information of the copied data packets in denying access to the data ports (see col. 9 lines 1-12).

As to claim 7, Cunningham teaches the method according to claim 6 wherein the step of using the protocol information further comprises storing in a memory the source addresses of the data packets traversing the data ports during the predetermined period of time (see col. 6 lines 49-67).

As to claim 8, Cunningham teaches the method according to claim 7 further comprising sorting the data packets traversing the data ports based upon the source addresses of each data packet (see col. 6 lines 49-67).

As to claim 9, Cunningham teaches the method according to claim 8 wherein the step of sorting further comprises creating a reference index having a number count for determining the number of data packets from each source traversing the data ports and incrementing the number count when subsequent data packets from the same source address traverse the data ports during the predetermined period of time (see col. 9 lines 1-12).

As to claim 10, Cunningham teaches the method according to claim 9 further comprising erasing from memory the reference index after the predetermined period of time expires (see col. 4 lines 31-44).

As to claim 11, Cunningham teaches the method according to claim 1 further comprising allowing data packets from sources other than the denied source to traverse the data ports (see col. 3 lines 56-col. 4 lines 5).

As to claim 12, Cunningham teaches the method according to claim 1 wherein the predetermined number of packets traversing the data ports and the predetermined period of time is configurable for each of the data ports (see col. 4 lines 32-43).

As to claim 13, Cunningham teaches a method of protecting a data network from data packets being sent from a suspicious source, the method comprising the steps of sampling the data packets and identifying a source that sends packets in excess of a predetermined number during a predetermined time (see col. 4 lines 32-43, col. 9 lines 1-12 and col. 3 lines 56-col. 4 lines 5).

As to claim 14, Cunningham teaches the method according to claim 13 further comprising excluding from the data network data packets transmitted from the identified source (see col. 6 lines 49-67).

As to claim 15, Cunningham teaches a method of protecting a network from data packets transmitted by a suspicious source, the method comprising the steps of sampling the data packets transmitted to and from the network, identifying any source that transmits data packets to and from the network in excess of a predetermined rate,

and automatically excluding from the network data packets from the identified source for a predetermined time (see col. 4 lines 32-43, col. 9 lines 1-12 and col. 3 lines 56-col. 4 lines 5).

As to claim 16, Cunningham teaches a system for protecting a network, the system comprising a monitoring means programmed for sampling data packets transmitted to and from the network, a memory for storing the sampled data packets and a processor for identifying sources transmitting data packets to and from the network in excess of a predetermined rate (see col. 4 lines 32-43, col. 9 lines 1-12 and col. 3 lines 56-col. 4 lines 5).

As to claim 17, Cunningham teaches the system according to claim 16 wherein the monitoring member is configured to exclude data packets transmitted to and from the network by the identified source (see col. 6 lines 49-67).

As to claim 18, Cunningham teaches the system according to claim 17 wherein the memory is configured to maintain a count of the number of data packets transmitted from any source to and from the network (see col. 9 lines 1-12).

As to claim 19, Cunningham teaches a computer running a plurality of packet daemons for monitoring the data ports of a network, each data port monitored by a separate packet daemon, and each packet daemon configured to identify any source that transmits data packets through its data port in excess of a predetermined rate resulting in the firewall excluding the data packets from the identified source (see col. 4 lines 32-43, col. 9 lines 1-12 and col. 3 lines 56-col. 4 lines 5).

As to claim 20, Cunningham teaches the computer of claim 19 further comprising a memory for storing the data packet count of transmitted data packets from any source (see col. 9 lines 1-12).

6.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Methods And Apparatus For A Computer Network Firewall With Cache Query Processing by Coss et al., U.S. Patent No. 6,170,012.

- Method And Apparatus For Defining And Implementing High-Level Quality Of Service Policies In Computer Networks by Gai et al., U.S. Patent No. 6,167,445.

- Method And Apparatus For Controlling Access To Services Within A Computer Network by Wong et al., U.S. Patent No. 5,835,727.
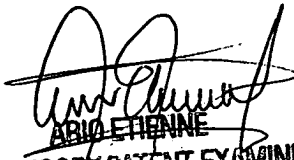
7.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hussein A El-chanti whose telephone number is (703)305-4652. The examiner can normally be reached on Mon-Fri 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (703)308-7562. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Hussein El-chanti

April 8, 2004

ABDU ETIENNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100